

Internal and Confidential

Netradyne Incident Management Process  
V2.2

Table of Contents

[Netradyne Incident Management SOP 0](#_Toc160727634)

[Document Control 2](#_Toc160727635)

[1 Purpose 3](#_Toc160727636)

[2 Scope 3](#_Toc160727637)

[3 Roles and Responsibilities 3](#_Toc160727638)

[4 Procedure 3](#_Toc160727639)

[4.1 Process Description, Process Goals, Objectives & Enablers 3](#_Toc160727640)

[4.2 Policies & Key definitions 4](#_Toc160727641)

[4.3 SLA Definitions & Priority Matrix 5](#_Toc160727642)

[4.3.1 Response & Resolution SLA 5](#_Toc160727643)

[4.3.2 Priority Definitions 5](#_Toc160727644)

[4.3.3 Incident Categorization Matrix 6](#_Toc160727645)

[4.3 Service Levels 7](#_Toc160727646)

[4.4 Key Contacts & Escalations Matrix 8](#_Toc160727647)

[4.5 RACI 8](#_Toc160727648)

[4.6 Incident Management Process Roles 9](#_Toc160727649)

[4.7 Incident Source & Workflow 10](#_Toc160727650)

[4.8 Incident Management Process Flow 11](#_Toc160727651)

[4.9 Incident Management Process Steps 11](#_Toc160727652)

[4.10 Incident Status 13](#_Toc160727653)

[4.11 Incident Contact Types 13](#_Toc160727654)

[4.12 Links with Change Management & Problem Management 14](#_Toc160727655)

[4.13 Three Strike Process 14](#_Toc160727656)

[4.14 P1 Notifications 14](#_Toc160727657)

[4.15 Interface with Other ITSM Processes 17](#_Toc160727658)

[5 Conduct 18](#_Toc160727659)

[6 Exception 18](#_Toc160727660)

[7 Terms/Acronyms 18](#_Toc160727661)

[8 Appendix A: Document RACI Matrix 19](#_Toc160727662)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDIM2024002 |
| **Document Name** | Netradyne Incident Management Process |
| **Document Status** | Released |
| **Document Released Date** | 05-Mar-2024 |
| **Document Author** | Priyesh Parashar |
| **Document Content Contributors** | Priyesh Parashar, Vijaykumar Dalal, Chethan G. |
| **Document Signatory** | saravanan.sankaran@netradyne.com |
| **Document Owner** | priyesh.parashar@netradyne.com |
| **Document Version** | v2.2 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| V1.0 | 26/08/2022 | Released | Vijaykumar Dalal |
| V1.1 | 22/06/2023 | Annual Revision | Chethan G. |
| V2.0 | 05/03/2024 | Major Changes in the contents | Priyesh Parashar |
| V2.1 | 22/03/2024 | Updated exception Section | Priyesh Parashar |
| V2.2 | 11/03/2025 | Updated Pending Status | Priyesh Parashar |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 26/08/2022 | Saravanan Sankaran | Sr. Director – Infosec & IT | Approved |
| 26/06/2023 | Saravanan Sankaran | Sr. Director – Infosec & IT | Approved |
| 05/03/2024 | Saravanan Sankaran | Sr. Director – Infosec & IT | Approved |
| 22/03/2024 | Saravanan Sankaran | Sr. Director – Infosec & IT | Approved |
| 14/03/2025 | Saravanan Sankaran | VP – Infosec & IT | Approved |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| Netradyne Leads | VPs, Directors, Functional Owners, Functional Leads |
|  |  |
|  |  |

# Purpose

This document covers a brief set of details around Incident Management on how the Incident Management process operates within Netradyne. It describes how Incident is triggered and handled using a structured process to restore the service as quickly as possible by minimizing the adverse impact on the business.

# Scope

Any event which disrupts, or which could disrupt, a service, including those reported directly by users, logged by technical staff, detected by event management tools, or reported by partners. Incident Management encompasses all IT service providers, internal and third parties, reporting, recording, or working on an Incident. All Incident Management activities should be implemented in full, operated as implemented, measured, and improved as necessary.

# Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Owner | * Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. * Is the point of contact for the document. * Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process. |
| Reviewers/Stakeholders | Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality) |
| Approvers | The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead. |
| Document Release | Document Owner/team to work with repository administrator to make release version available. |

# Procedure

The purpose of the Incident Management Process document is to provide end-to-end context for the Incident Management Process. This document serves as an official process to be used by the Netradyne Support team, while supporting the business. It introduces a Process-Framework and contains the workflow, roles, procedures, and policies needed to implement a high-quality process and ensure that the processes are effective in supporting the business.

# 4.1 Process Description, Process Goals, Objectives & Enablers

**Process description**: An incident is defined as an unplanned interruption or a reduction in the quality of an IT service or a failure of a configuration item (CI) that has impacted the IT service. Incidents can include failures or degradation of services reported by users, technical staff, third-party suppliers and partners, or automatic failures from monitoring tools. Incident management is responsible for managing the entire lifecycle of all incidents.



**Process Goals**: The Incident Management process within Netradyne is designed to restore a service as quickly as possible with minimal disruption to the business, possibly by using workaround solutions. Incident management process ensures that best possible levels of service quality and availability are maintained.

Incident Management is not concerned with ‘fixing’ the underlying problem (root cause) of the incident; this is managed by Problem Management. It simply restores End Users to an agreed service level in the fastest way possible, by whatever available means – this may include employing use of final resolution or temporary fixes or workarounds.

**The objectives** of the incident management process are to:

* To restore service operations as quickly as possible.
* Align incident management activities and priorities with those of the business while maintaining user satisfaction with the quality of IT services.
* Ensure that standard methods and procedures are used for efficient and prompt incident handling viz., response, analysis, documentation, ongoing management, and reporting.
* Increased visibility and communication of incidents to business and support staff.
* Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents, as and when they occur.

**Enablers of Objectives**: The objectives are achieved by:

* Structured approach to log, diagnose and resolve incidents.
* Clearly priorities that relate to (business) impact and have a business orientation.
* Improved knowledge management.
* Clear link between Problems and Changes.
* Underpinning governance and continual improvement of the process.

# 4.2 Policies & Key definitions

Incident Management policies are required to make all staff aware of the steps needed to make Incident Management effective. They address the following:

* One standard Incident Management process is defined and used to support all IT service users.
* All MI should be notified into SD+
* All incidents must be logged, prioritized and solutions recorded in the Incident Management System (use of a single service management system for all incidents).
* Incident Management should be aligned with overall service levels and objectives.
* The Incident Management process is the channel of communication for any degradation of service, to the affected users and IT personnel.
* Hierarchical escalations for appropriate IT management notifications.
* Routine audits of incident records to ensure correct incident categorization and documentation.
* Incident reporting must go through the IT Support Team, providing users with a single point of contact.
* The IT Support Team manages, tracks, escalates, closes, and communicates the status of all incident records and is responsible for all incident assignments.
* Closure of incidents is dependent on validating with the user, that the incident has been resolved, and that the service is restored.

# 4.3 SLA Definitions & Priority Matrix

# 4.3.1 Response & Resolution SLA

|  |  |  |
| --- | --- | --- |
| Priority Level | Response Time | Resolution Time |
| P1 | 15 Mins | 4 Hours |
| P2 | 2 Business Hours | 8 Business Hours |
| P3 | 8 Business Hours | 2 Business Days |
| P4 | 12 Business Hours | 4 Business Days |

# 4.3.2 Priority Definitions

**Major Incident** means an Incident that meets the criteria set out in “Priority 1 (Critical)” or “P1” in this table that triggers the major incident management process.

**Priority 1 Incident**: means an Incident that meets one or more of the following criteria:

* A critical service, business unit or business function is unavailable.
* A critical service, business unit or business function unable to operate or not operating correctly.
* The issue is severely impacting or affecting multiple users and / or multiple functions and / or multiple sites.
* The business operations are severely impacted or not possible.
* There is or may be serious business or financial exposure, including but not limited to significant potential revenue loss.

Examples include, but are not limited to:

* Critical systems component failed or severely impaired at any site.
* multiple server failures affecting key operational areas of the Customer's businesses.
* severe degradations in performance.
* health and safety could be at risk.
* financial systems impacted in a financial close period.

**Priority 2 Incident**: means an Incident that meets one or more of the following criteria:

* Causes major business disruption.
* Multiple users are unable to operate or perform some significant portion of their job.
* A business unit or department is experiencing significant reduction in systems performance.
* There is the potential to cause or become a P1 Incident
* There is or may be serious business or financial exposure, including but not limited to significant potential revenue loss.

Examples include, but are not limited to:

* Loss of Service affecting five (5) or more users.
* Loss of Service affecting between two (2) and five (5) users in the same department/location.
* Slow response of a key business application, experienced by one or more users, that reduces operational efficiency and inconveniences users;
* Events triggered on servers related to any performance, however under Threshold limits.

**Priority 3 Incident**: means an Incident that meets one or more of the following criteria:

* Impacts the services or operations resulting in non-availability or incorrect operation affecting a single user or small number of users (that is less than five (5), not in the same department or location).
* Workarounds may be in place and business operations are impacted, although not severely.
* Equipment failures where, due to redundancy and resilience arrangements, service is unaffected.
* Issues that would restrict or damage the business if not resolved within the agreed timescale.

Examples include, but are not limited to:

* common user issues e.g., being unable to use email, to print, logon etc.
* password resets.
* computing device (i.e., hardware) of a single user not working.
* an application user profile/account not having the agreed permissions as agreed in the Customer's Requirements.
* Events triggered on production servers related to any performance, however under warning limits.

**Priority 4 Incident**: means an Incident which causes minor disruption which:

* Issue causing an inconvenience.
* Impacts a single user or smaller user group but those users are still able to perform the majority of their duties.
* The business operations are not impacted.
* There is no financial impact for the Customer.
* Performance of systems is delayed but still functioning. Bug affects a small number of users. Acceptable workaround available

Examples include but are not limited to:

* Requests for information.
* User queries as to how to carry out a function.
* Joiner/Mover and Leaver “how to” requests.
* Events triggered on non-Production servers related to any performance, however under warning limits.
* Website is slow in responding to requests.

# 4.3.3 Incident Categorization Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Priority Matrix** | | **Impact** | | |
| **Global** | **Multiple Users/Regions** | **Single User** |
| **Urgency** | **Unavailable** | 1 | 2 | 3 |
| **Performance Issues** | 2 | 3 | 4 |
| **Functionality** | 3 | 4 | 4 |

# 4.3 Service Levels

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Service Level Name** | **Expected** | **Minimum Service Level (Threshold)** | **Service Level Calculation** |
| **SLA 01** | Major Incident Response | 15 minutes | 90% | Service Level achieved = (MI15 / TMI) x 100 where: “MI15” means total number of P1 Incidents responded in fifteen (15) minutes; and “TMI” means total number of P1 Incidents closed in the month. Exclude Incidents which are cancelled. |
| **SLA 02** | Major Incident Resolution | 4 Hours | 90% | Service Level achieved = (IR / TI) x 100 where: “IR” means total number of Major Incidents resolved within four (4) hours; and “TI” means total number of Major Incidents resolved in the month. Resolution is Met when the ticket moves in “Closed State” post 5 business days of being marked as Resolved. |
| **SLA 03** | P2 Incident Response | 2 Hours | 90% | Service Level achieved = (P2 30 / TP2) x 100 where: “P2 30” means total number of P2 Incidents responded to in one (2 hours); and “TP2” means total number of P2 Incidents closed. Exclude Incidents which are cancelled. |
| **SLA 04** | P2 Incident Resolution | 8 Hours | 90% | Service Level achieved = (RP2 / CI) x 100 where: “RP2” means total number of P2 Incidents resolved within eight (8) hours; and “CI” means total number of P2 Incidents closed in the month. Resolution is Met when the ticket moves in “Closed State” post 5 business days of being marked as Resolved. |
| **SLA 05** | P3 Incident Responses | 8 Hours | 85% | Service Level achieved = (P3 2 / TP3) x 100 where: “P3 2” means total number of P3 Incidents responded to in four (8) hours; and “TP3” means total number of P3 Incidents closed. Exclude Incidents which are cancelled. Response is Met when a ticket is assigned to the relevant resolver group |
| **SLA 06** | P3 Incident Resolution | 2 Days | 85% | Service Level achieved = (P3 2 / TP3) x 100 where: “P3 2” means total number of P3 Incidents resolved within two (2) Business Days; and “TP3” means total number of P3 Incidents closed in the month. Resolution is Met when the ticket moves in “Closed State” post 5 business days of being marked as Resolved. |
| **SLA 07** | P4 Incident Response | 12 Hours | 85% | Service Level achieved = (P4 4 / TP4) x 100 where: “P4 4” means total number of P4 Incidents responded to in eight (12) hours; and “TP4” means total number of P4 Incidents closed in the month. Exclude Incidents which are cancelled. Response is Met when a ticket is assigned to the relevant resolver group |
| **SLA 08** | P4 Incident Resolution | 4 Days | 85% | Service Level achieved = (P4 7 / TP4) x 100 where: “P4 7” means total number of P4 Incidents resolved within four (4) Business Days; and “TP4” means total number of P4 Incidents closed in the month. Resolution is Met when the ticket moves in “Closed State” post 5 business days of being marked as Resolved. |

# 4.4 Key Contacts & Escalations Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Contact** | **Email ID** | **Role** |
| Priyesh Parashar | 9845227014 | [priyesh.parashar@netradyne.com](mailto:priyesh.parashar@netradyne.com) | Staff Manager – ITSM |
| Saravanan Sankaran | 9444161422 | [saravanan.sankaran@netradyne.com](mailto:saravanan.sankaran@netradyne.com) | VP - Info Security & IT |

# 4.5 RACI

This section maps the Roles and Responsibilities to the various steps in the workflow.

* Responsible: Those who do the work to achieve a task. There is typically one role with a participation type of Responsible.
* Accountable: Those who are ultimately accountable for the correct and thorough completion of the deliverable or task, and the one to whom Responsible is accountable. Typically, the process owner is Accountable for a process, and there must be only one Accountable specified for each task or deliverable.
* Consulted: Those who are not directly involved in the process but provide inputs and whose opinions are sought.
* Informed: Those who receive outputs from the process or are kept up to date on the progress, often only on completion of the task or deliverable

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activity | IT Support Analyst | Process Owner | Incident Manager | User |
| Phase 1: Incident Identification & Logging | | | | |
| 1.1 Log new Incident | R,C,I | C | I,C | A |
| 1.2 Provide incident summary, CI | R,C,I | C | I,C | A |
| 1.3 Select Urgency | R,C,I | C | I,C | A |
| 1.4 Assign Incident to Support Group | R | I,C | A | I |
| Phase 2: Incident Classification & Prioritization | | | | |
| 2.1 Review Incident Information | R | C | A | I,C |
| 2.2 Assign incident to a technician | R | C | A | I |
| 2.3 Reassign incident | R | C | A | I |
| 2.4 Duplicate Incident | R | C | A | I,C |
| 2.5 Escalate Incident? | R | C | A | I |
| Phase 3: Incident Investigation & Diagnosis | | | | |
| 3.1 Major Incident | R | C | A | I |
| 3.2 Solution Found in Knowledgebase? | R | C | A | I |
| 3.3 Incident caused by Change? | R | C | A | I |
| 3.4 Relate incident to change | R | C | A | I |
| 3.5 Resolution Found? | R | C | A | I |
| 3.6 Document solution (if doesn’t exist) | R | C | A | I |
| Phase 4: Incident Resolution & Closure | | | | |
| 4.1 Resolve without change | R | C | A | C |
| 4.2 Implement Resolution | R | C | A | I,C |
| 4.4 Verify & confirm resolution | R | C | A | I,C |
| 4.5 Resolve incident | R | C | A | I |
| Phase 5: Incident Monitoring | | | | |
| 5.1 Any open incidents with SLA? | R | C | A | I |
| 5.2 SLA breached | R | C | A | I |
| 5.3 Escalation Required? | R | C | A | I |

# 4.6 Incident Management Process Roles

Each role is assigned to perform specific tasks within the process. Within a specific process, there can be more than one individual associated with a specific role. Additionally, a single individual can assume more than one role within the process although typically not at the same time. Depending on the structure and maturity of a process, all roles described may not exist in every organization.

The following table describes the typical roles defined for Incident Management:

| **Role** | **Description** |
| --- | --- |
| **Incident Management Process Owner** | A Senior Manager with the ability and authority to ensure the process is rolled out and used by the entire IT organization.  **Responsible for:**   * Defining the overall mission of the process. * Establishing and communicating the process mission, goals, and objectives to all stakeholders. * Resolving any cross-functional (departmental) issues, including resource availability. * Ensuring consistent execution of the process across the organization. * Reporting on the effectiveness of the process to senior management. * Initiating any process improvement initiatives. |
| **User** | **Responsible for:**   * Bringing incidents to the attention of the IT Support Team. * Providing Incident description with accurate information * Participating in the implementation (of a solution) and resolution or workaround and verifying correct operation once implemented, as needed. * Incident closure confirmation |
| **IT Support Team** | **Responsible for:**   * Recording (logging), ownership, monitoring, tracking, and communication about incidents. * Response SLA, if assigned to IT Support Team * If a User logs a Major Incident, SD to validate with Incident Manager * Update Front end message on SSP. * Investigating and diagnosing incidents. * Providing resolutions and workarounds from standard operating procedures, knowledge base articles and existing known errors. * Escalating incidents to appropriate incident support teams. * Routing of Incident to next level of support if a resolution cannot be identified. * Responsible for the Response SLA of P1/P2/P3/P4 Incident (assigned to SD) * Tagging/linking all the non-MI tickets related to major Incident and keeping the Incident status in On-Hold status. * Confirm resolution status of P1 with end users. * Verifying resolution confirmation (MI & Non-MI) * Developing workarounds and submitting knowledge articles. * Escalating issues to management as appropriate / applicable during resolution. * Raising a change if resolution requires one. * Engaging Vendor / Vendor management wherever vendor assistance is required. * Seek approvals from delegates to implement changes to fix the issue. |
| **Incident Manager** | **Responsible for:**   * Process compliance check. * Review the Pending & WIP incidents. * Managing the day-to-day activities of the process. * Driving the efficiency and effectiveness of the Incident Management process. * Gathering and reporting on process metrics. * Developing and maintaining the process procedures. * Manage major incident P1. * Ensure P1 is fixed with defined SLA. |
| **IT Support Manager/ Lead** | **Responsible for:**   * Managing resources assigned to the IT Support Team. * Managing Service Desk activities. Provides guidance to IT Support team members. * Monitoring and reporting on IT Support Team performance. * Taking overall responsibility for incident and service request handling by the IT Support Team. * Making improvements to the IT Support Team. |

# 4.7 Incident Source & Workflow

A diagram of a event monitoring

Description automatically generated

* Users can report issues to IT Support Team via emails, call and self-service portal.
* Incidents captured during event monitoring.
* Users can log incidents via self-service portal.

# 4.8 Incident Management Process Flow

A diagram of a flowchart

Description automatically generated

# 4.9 Incident Management Process Steps

| Step | Description | Role |
| --- | --- | --- |
| 1 | **Issue detected**  End users experience Outage/downtime /degradation of services | User / Caller |
| 2 | **Report to IT Support Team**  End users can drop an email or raise an incident through SSP to IT Support Team to report the Outage/downtime /degradation of services | User/Caller |
| 3 | **Initial diagnosis**  IT Support Team needs to assess & see if the issue reported by user qualifies for a service request/ incident/major incident | IT Support Team |
| 4 | **Is this a Service Request?**  IT Support Team should identify if the caller’s need can be satisfied by one or more of the existing Service Requests.  If yes, then the IT Support Team will guide them on logging SRs/ convert the existing ticket to Service Request  If no, then the IT Support Team will move to classify and prioritize the incident  **Instead of raising a Service Request, end user raises an Incident ticket:**   * IT Support Team should convert the incident to service request * Post converting to a SR, inform the end user that we have converted the incident and also educate the end user about the difference between incident & a service request   **Difference between Incident & Service Request**:   * Incident: Restoring something that is broken/disrupted. Examples include fixing a printer, phone, or software. * Service Request: Fulfilling a request for information/advice or access a Service. Examples granting access to a printer or providing standard setup Services for a new employee or installation of new applications for the first time. | IT Support Team |
| 5 | **Classify and prioritize Incident**  IT Support Team classifies the Incident according to prioritization models  IT Support Team should refer the solutions if there are any details captured regarding how the incident needs to be handled in case this is identified as a repeat incident.  When prioritizing incidents and service requests, IT Support Team must take into consideration the live impact of the incident or service request at that point in time. | IT Support Team |
| 6 | **Request Fulfillment process**  If the record is identified as Service Request during categorization, the record is handed over to Request Fulfilment Process | IT Support Team |
| 7 | **Assign to respective Resolver group**  IT Support Team triage or assign the incidents to the respective resolver group queue for restoration of services | IT Support Team |
| 8 | **Is it a Major incident?**  After assessment, if the incident falls in major incident category, MIM process to be initiated. The Major Incident management process will drive the incident to closure and all action henceforth will be undertaken as per the dictates of that process | IT Support Team |
| 9 | **Invoke Major Incident Management process**  Incident Manager will initiate the Bridge, Notifications/SMS & Callout respective support groups to ensure the services the restored at the earliest. | Incident Manager |
| 10 | **Diagnose Incident**  Support teams use their skills to diagnose the issue. Investigative techniques, pre-ordained scripts and SOPs can be used to restore the services as soon as possible.  Escalations across groups and levels will happen at this stage as required.  In this step, the entire team puts together their skills and acumen to investigate the incident and come up with a resolution. Once, the resolution is known,  Resolver group needs to check the CMDB service map, solutions, check Recent changes on Infra / Application CIs for potential resolution | Resolver group |
| 11 | **Provide Workaround**  A workaround is used for Reducing or eliminating the impact of an incident for which a full resolution is not yet available. Workarounds for incidents that do not have associated problem records are documented in the incident record.  **Provide Permanent fix**  A permanent fix is one that completely resolves the underlying Problem by eliminating its root cause. It prevents any more Incidents from being caused by the said Problem. | IT Support Team |
| 12 | **Incident resolved?**  Check if the incident is resolved – unresolved incidents are escalated according to the escalation matrix and sent back for fresh diagnosis and resolution attempts by escalating to the next level or involving Vendor management (wherever applicable).  The escalation matrix will establish Vertical escalation levels in the form of L1, L2, L3 – Vendor and Horizontal escalation levels across resolver groups for specialized domains | IT Support Team |
| 13 | **Escalate per escalation matrix**  In case the resolver group is unable to diagnose the issue, they must escalate according to the escalation matrix. By escalation, they can involve either peer groups with different areas of expertise or higher authorities with greater scope of visibility.  Escalation brings in a fresh perspective from peer groups or higher levels of visibility from the higher authorities and contributes to quicker resolution of the incident.  **Invoke Vendor management**  Support teams to involve Vendors through respective service owner/BU Heads. | IT Support Team |
| 14 | **Communicate & Confirm resolution with User**  Mostly, an email is sent out on behalf of the IT Support Team by the tool itself.  This communication should follow the pattern of the 3-strike rule.  Team will initiate closure communication with user by indicating resolution and getting user feedback. It is important to keep the questions neutral while asking user’s opinion. The last question should always be open, like: “Is there anything you would like to say?” which will allow the user to voice out any other hindrances in their usage of services | IT Support Team |
| 15 | **Document the Restoration steps**  Resolver groups involved in the service restoration need to capture the diagnosis & restoration activities performed | IT Support Team |
| 16 | **Resolve**  The status of the incident is set as “resolved” and assigns the closure-category to each incident.  While closing the incident the respective resolver group needs to mark the closure category of the incident which is the real category in which the incident was closed regardless of the initially assigned category. This is very important for reporting on incident management process. | IT Support Team |

# 4.10 Incident Status

|  |  |
| --- | --- |
| State | Description |
| New | Incident is logged but not yet investigated |
| In Progress | Incident is assigned and is being investigated. Technician is working on to fix the issue. |
| On Hold | The responsibility for the incident shifts temporarily to another entity to provide further information, evidence, or a resolution. Refer the table below for the On-Hold Reasons |
| Resolved | A satisfactory fix is provided for the incident to ensure that it does not occur again |
| Closed | Incident is marked Closed after it is in the Resolved state for a specific duration, and it is confirmed that the incident is satisfactorily resolved |
| Canceled | Incident was triaged but found to be a duplicate incident, an unnecessary incident, or not an incident at all |

The On-Hold state is further classified into below 4 On Hold Reasons. SLA will get paused on below status.

|  |  |
| --- | --- |
| State | Description |
| On Hold - Awaiting Additional Approval | Ticket that is waiting for the additional approval from various approvers |
| On Hold - Awaiting Approval | Ticket that is waiting for the approval from various approvers |
| On Hold - Awaiting Asset Return | Status indicating a task is paused pending the return of company-owned assets |
| On Hold - Awaiting Change/Onboarding/Offboarding | Status indicating a task is paused pending completion of a change request or onboarding/offboarding process. |
| On Hold - Awaiting Requester | A ticket that is temporarily paused or delayed, often waiting for additional information from the user |
| On Hold - Awaiting Vendor/Another Team | Status indicating a task is paused pending input or action from a vendor or another team |

# 4.11 Incident Contact Types

|  |  |
| --- | --- |
| Method | Description |
| Email | User has reported an issue by sending email to [itservicedesk@netradyne.com](mailto:itservicedesk@netradyne.com) |
| Phone | User has reported an issue over phone call |
| Self-Service | User has reported an issue or submitted request via ServiceDesk+ User Portal |
| Walk-In | User has reported an issue by visiting IT technician in office and IT Technician has submitted the ticket |

# 4.12 Links with Change Management & Problem Management

* All incidents occurring due to change or that require change to resolve the underlying issue would be tagged to the change field in SD+.
* For repetitive incidents in the environment, problem ticket would be raised and assigned to problem management team for further analysis.
* For all the P1 incidents, problem ticket would be generated to find out the root cause.

# 4.13 Three Strike Process

The Three strike rule needs to be applied when Incident analyst may try to reach the user to confirm service has been restored or if there is no response from user on the information that has been requested. When a service request or customer-initiated incident is resolved, communication with customer is required for confirmation of closure.

Follow the below steps:

Post Incident resolution send an email communication on each working day to seek confirmation from User on resolution provided.

* Update case log in the tool on each follow-up. State clearly on the mails that the case will be closed after the 3rd communication attempt.
* Users would be contacted via 2 different modes of communication while applying 3 strike process. (Eg: phone, email, chat, etc)
* Mark each attempt as Reminder#1 or Reminder #2 or Reminder #3. (On 3 different days)
* In case of VIP user try to reach over personal phone number.
* After 3rd strike if no user response received, the analyst can close the ticket with appropriate closure code. (Note: Once you send the 3rd strike wait for 24 hours for response)
* In case the user is out of office or has set automatic response for return on specific analyst need to wait for his return or should reach out to the delegate set by the user.
* If the user/delegate informs that he would not be available to confirm the issue status in next 5 days, such cases would be discussed with IT Support Team manager/lead team for future course of action/resolution/cancellation.
* Three strike rules do not apply to Major incident raised.

# 4.14 P1 Notifications

To ensure the effective communication being followed for high priority incidents for the organizations IT Services, this document provides the guidelines for High Priority Incident Communications.

* **Responsibilities**

The IT Team support will send out the communications to all the stakeholders of the organization

IT Team will:

1. Follow the defined template to send the communication for all the critical/high priority issues as per defined frequency.
2. The template will be only sent to Netradyne Users
3. Adhere to the guidelines provided in the Procedure section
4. Respond to any queries from the stakeholders

ITSM Analyst:

1. Ensure the communication are sent by the support lead as defined & monitor the same
2. Respond to any escalations related to the issues

* **Timeline and Recipients**

|  |  |
| --- | --- |
| **Status** | **Timeline** |
| Open | Within 30 Mins of issue re-occurred |
| In Progress | Every 2 Hrs. |
| Closure | Within 60 Mins |

|  |  |  |
| --- | --- | --- |
| **Team** | **Recipients** | **Email Address** |
| All Users | All Netradyne Users | all@netradyne.com |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **Service Status: Unavailable/Degraded/Restored**  **Service Name:** | | | | | | | | | | | |  | | | | | | | | | | | | **Issue Description:** | *<<Provide the issue description in short>>* | | | | | | | | | | | **Ticket Number:** | *<<Update ServiceDesk+ Ticket ID>>* | **Priority:** | | | | | *<<Update Priority of the Ticket>>* | | | | | **Location Impacted:** | *<<India or US or Global>>* | **IT Analyst:** | | | | | <<Update IT Analyst Name>> | | | | | **Business Impact:** | *<<Provide the business impact due to the issue>>* | | | | | | | | | | | **No. of Users Impacted:** | *<<Provide the number of users impacted approx..>* | | | | | | | | | | | **Start of Impact:** | *<<Provide the date & time when the issue occurred in GMT>* | **Issue Restored At:** | *<<Provide the date & time when the issue was restored in GMT>* | | | | | | | | | **Workaround:** | *<<Provide if there is any workaround in place>>* | | | | | | | | | | | **Actions Completed:** | **Final Update:**   * <<Provide the updates in bullets>>   **Update 3:**   * <<Provide the updates in bullets>>   **Update 2:**   * <<Provide the updates in bullets>>   **Update 1:**   * <<Provide the updates in bullets>> | | | | | | | | | | | **Next Actions:** | *<<Provide the next actions to be taken to troubleshoot or resolve >>* | | | | | | | | | | | **Next Update:** | *<<Provide the date & time when the next update will be sent>>* | | | | | | | | | | | **External Dependency:** | *<<Provide name of vendor if any involvement>>* | | | | | | | | | | | **Manager:** | * priyesh.parashar@netradyne.com * [saravanan.sankaran@netradyne.com](mailto:saravanan.sankaran@netradyne.com) | | | | | | | | | | | **Resolution:** | *<<Provide the resolution steps in brief>>* | | | | | | | | | | |  |  |  | |  |  |  | |  |  |  | |   Please reach out to [it@netradyne.com](mailto:it@netradyne.com) if more information required on this issue. |

***This communication has been sent per Bcc to:***

*<<Provide Email IDs for which the communication to be sent>>*

* **Banner Heading:**

1. **Service Status: Unavailable/Degraded/Restored/Monitoring**

* Unavailable – If IT service/application is completely inaccessible/unavailable. The banner colour should be AMBER
* Degraded – If some functionality of IT service/application is not working or there is a performance issue. The banner colour should be AMBER
* Restored – If the issue is resolved or restored. The banner colour should be GREEN

1. **Service Name:** Update the impacted IT service or application name

* **Banner Description:**
* **Issue Description** - Summarize about the issue reported by user
* **Location Impacted** - Mention all the countries/location/sites impacted
* **IT Analyst –** Update the name of the IT Team Analyst who is working on the issue
* **Business Impact** – Update the business impact due to the reported issue (Business centric description)
* **No. of** **Users Impacted** – Update number of users impacted across all location/Site
* **Start of Impact** – Update the date and time in GMT when issue was first observed
* **Issue Restored At** – Update date and time in GMT when issue was resolved
* **Workaround** –Update the workaround solution is available else mention **No Workaround**
* **Actions Completed** – Provide the steps of the action taken from previous communication to current progress made & continue the same till resolution. Greyed out the previous updates
* **Next Actions** – Provide the next set of actions along with action owner (team name) if the Investigation/troubleshooting is in progress
* **Next Update** – Update the date & time in GMT by when the next update on the issue will be provided to the stake holders
* **External Dependency** – Update the names of 3rd party/middleware’s/infra teams along with ticket number opened for them
* **Email Message:**
* **Subject:** Major Incident | Service or Application Name | Issue Description
* **From:** Theemail must be sent from IT & InfoSec mailbox
* **To:** Provide your team email address so that for any queries, available person can revert
* **Bcc:** Include the below recipient’s email address for all the comms and along with that add Email Ids for which the communication banner to be sent

# 4.15 Interface with Other ITSM Processes

| Process | Relationship Description | Input | Output |
| --- | --- | --- | --- |
| Request Fulfilment | If the record is identified as Service Request during categorization, the record is handed over to Request Fulfilment Process |  | X |
| Problem Management | Problems can be initiated from an incident when determining the root cause of the incident needs further investigation.  Incident information is proactively analysed to detect trends in service behaviour that may be indicative of an underlying problem. |  | X |
| Information about known errors and their workarounds is used to diagnose and resolve recurring incidents faster. | X |  |
| Change Management | A request for change (RFC) can be submitted to implement a workaround or a resolution. |  | X |
| Can detect and resolve incidents that arise from changes.  Change management is responsible for keeping the Service Desk informed of all scheduled changes. | X |  |
| Service Level Management  (SLM) | Defines measurable responses to service disruptions.  Provides historical data that enables SLM to review service level agreements (SLAs) objectively and regularly.  Assists SLM in defining where services are at their weakest so that SLM can define actions as part of the service improvement plan (SIP). | X | |
| Knowledge Management | Knowledge Management provides knowledge information and related documentation to Incident Management to support Incident Resolution | X |  |
| Configuration Management | Incident Management Queries Configuration Management to identify reported, affected and failing CIs relating to an incident/outage | X |  |
| Incident Management | A request for change (RFC) can be initiated when a CI change is required to resolve an incident. | X |  |
| Change management is responsible for keeping the service desk informed of all scheduled changes.  Access to recent change information can be used to determine the cause of current incidents. |  | X |
| Problem Management | Problem management is informed of the status and progress of submitted RFCs. |  | X |
| Release Management | Release deployment plan may be required for implementing a change |  | X |
| Service Request Management | Requests for change (RFCs) may be needed to complete fulfilment actions for certain types of service requests. | X |  |

# Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non-compliance will be escalated to the Netradyne leadership team.

# Exception

Currently, there is no exception on incident management process. All break-fix issues should be reported via incident tickets only. Service requests are not the appropriate channel for addressing break-fix problems.

If an end user submits a service request for a break-fix issue, the engineer is required to convert the service request into an incident ticket and proceed accordingly. This ensures efficient handling and resolution of technical issues.

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| **Capability** | The ability of an organization, person, process, application, IT service or other configuration item to carry out an activity. Capabilities are intangible assets of an organization. |
| **CI** | Configuration Item: Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management. They typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and service level agreements. |
| **CSI** | Continuous Service Improvement |
| **Incident** | An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident – for example, failure of one disk from a mirror set. |
| **IT** | Information Technology |
| **ITSM** | Information Technology Service Management |
| **Known Error** | A problem that has a documented root cause and a workaround. Known errors are created and managed throughout their lifecycle by problem management. Known errors may also be identified by development or suppliers. |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedure |
| **WLI** | Work Level Instructions |

# Appendix A: Document RACI Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Role/Activity | Document Owner/Functional Area Lead | Document Contributor | ND Leadership | Functional Area Team | InfoSec | All ND Member(s) |
| Ensure document is kept current | A | R | I, C | R, C | C | I |
| Ensure stakeholders are kept informed | A | R | - | R | C | - |
| Ensure document contains all relevant information | A | R | I, C | R, C | C | I |
| Ensure document adheres to document governance policy | A, R | R | I | R, C | R, C | I |
| Provide SME advice | I, R | A, R | I | R, C | I, C | I |
| Gathering and adding document contents | I | A, R | I, C | R, C | C | I |
| Document Approval | A | R | I, R | I | I, R | I |

|  |  |
| --- | --- |
| Key |  |
| R | Responsible |
| A | Accountable |
| C | Consulted |
| I | Informed |